cdgrf 43

Smart Card

Stage 1 Description

(Version 1.1)

May 22, 1996

CDMA Development Group

Smart Card Team Document

Please contact:

Narisa Chu, Comcast Cellular, Wayne, PA
610-995-5278, Fax: -5224
METROPHONE/WAYNE/NCHU%Comcast_Metrophone@mcimail.com

Cheryl Johnson, U S Cellular, Chicago, IL
312-399-8964 Fax: -4984
Cheryl_Johnson_at_USCC__P3@cellular.uscc.com

1. Introduction

This document presents Stage 1 descriptions for CDMA smart card services. The intent of this document is to provide inputs on user considerations, and possible service interactions to aid in the development of smart card services and other layer associated capabilities.

Smart card functionality includes:

- Privacy key management and authentication interface between the subscriber and the CDMA mobile station
- Personalized feature subscription record
- Transport of non-telephony applications, e.g. credit card, electronic coin purse and loyalty program
- Remote management of data/voice/facsimile applications.

Smart card applications are identified below:

- Pre-paid Services
- Plastic Roaming
- Fraud Prevention
- Future applications: Portable Storage and Non-telephony Services

It is assumed one card per subscription at the initial stage. Ultimately, there can be multiple cards per subscriber and the smart card can enable the wireless data/voice services as the transport mechanism underlying non-telephony, end-to-end applications.

With the above functions and applications, service providers will be able to realize the following benefits:

1) Service offers with billing and provisioning capabilities through an intelligent/synergistic mechanism.

2) Common/flexible means for billing and provisioning cross wireline, wireless, and cable TV services.

3) Plastic roaming cross different access technology networks.

4) Service portability for subscribers, subscriptions, network technologies, and service providers.

5) Marketing differentiation - Brand exposure, expanded distribution channels, advertising revenues, customer loyalty programs.

6) Billing and customer care alternatives - Fraud protection/management, ease of distribution, remote activation alternative.

7) Cheaper to subsidize if needed: cost per card is much cheaper than cost per mobile station.

8) Revenue assurance with pre-paid service.

The smart card can bring the following benefits to the subscribers:

1) Convenience for international business travel with rental mobile stations.

2) Domestic travel to areas with different network technology.

3) Public mobile stations with individual billing report.

4) Employees can share mobile stations with personalized privileges and accounting.

5) Family members can share a mobile station with cards tailored to specific needs and individual accounting.

6) It is easier to carry a plastic card than a mobile station.

7) Theft-proof : a smart card can not be used without a CHV verification and other security mechanism built in the network, e.g. IS-41 CAVE, etc.

8) Effective fraud control and prevention.

2. References

2.1. References for Smart Card Services

International Standards Organization (ISO) 7816-1,2,3-6 ***Information technology - Identification cards - Integrated circuit(s) cards with contacts*** **parts 1 through 6**

T1P1.3/V. 5.x ***PCS User Identity Module (UIM) Specification, 1996***

CCITT 1988 (Blue Book),Volume III - Fascicle III.7, ***Integrated Services Digital Network (ISDN) General Structure and Service Capabilities; Recommendations I.110 - I,257.***

Technical Specification GSM 02.17: ***Subscriber Identity Module, Functional Characteristics; August 31, 1993.***

Technical Specification GSM 11.11: ***Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; October 1993.***

J-STD-007, ***PCS 1900 Smartcard - ANSI Standard***

J-STD-008-1995, ***Personal Station-Base Station Compatibility***

ANSI Requirements ***for 1.8 to 2.0 GHz Code Division Multiple Access (CDMA)***

Personal Communications Systems ***, Telecommunications Industry Association, 1995.***

TIA/EIA/IS-41-C, ***Cellular Radio-Telecommunications Intersystem Operations, Telecommunications Industry Association, December 1995.***

TIA/EIA/IS-95-A, ***Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System, Telecommunications Industry Association, May 1995.***

TIA/EIA/IS-95-A, ***Appendix A, Message Encryption and Voice Privacy. An ITAR controlled document subject to restricted distribution. Contact the Telecommunications Industry Association, Washington, D.C., November 16, 1994.***

TSB50, ***User Interface for Authentication Key Entry, Telecommunications Industry Association, March 1993.***

TSB74, ***Support for 14.4 kbps Data Rates and PCS Interaction for Wideband Spread Spectrum Cellular Systems, Telecommunications Industry Association, December 1995.***

3. Definitions

Authentication - A secure procedure used to validate a mobile station's identity involving the A-key and the CAVE Algorithm.

Authentication Center - An entity that manages the authentication information related to the mobile station.

Authentication Key (A-key) - A secret 64-bit pattern stored in the subscriber unit. It is used to generate and update the subscriber unit's Shared Secret Data. The A-key is used in the authentication process.

Authenticating Network - Networks that validate a subscriber through authentication.

Authorized Dealer - An agent that is authorized by a service provider to sell that service provider's product or service to a customer.

Automatic Teller Machine (ATM)

Call - A temporary communication between telecommunications users for the purpose of exchanging information. A call includes the sequence of events that allocates and assigns resources and signaling channels required to establish a communications connection.

Card Holder Verification (CHV) - Access condition used by the SIM for the verification of the identity of the user.

Cellular Service Provider -A licensee of the responsible government agency (in the U.S., a licensee of the Federal Communications Commission) authorized to provide Cellular Radiotelephone Service.

Code Division Multiple Access (CDMA) - A technique for spread-spectrum multiple-access digital communications that creates channels through the use of unique code sequences.

Country Code - A unique 1-, 2- or 3-digit code assigned to countries in the World Numbering Plan. For international dialing purposes, the world is divided into nine zones. The first digit of a country code is the world number.

Customer - A person who purchases a mobile station and is a prospective subscriber to a cellular service provider.

Customer Service Center- An entity of a service provider that provides user support and assistance to subscribers.

Customer Service Representative - A person that operates from a customer service center and provides user support and assistance to subscribers.

DMH - Data Message Handler

Digits - Digits consist of decimal integers 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9.

Distribution Channel - A method for providing a product or service to a specific market.

Directory Number - The phone number used to dial a subscriber.

Dual-mode Mobile Station - A mobile station capable of analog or digital operation.

Electronic Serial Number (ESN) - A 32-bit number assigned by the mobile station manufacturer used to identify a mobile station. The ESN is unique for each legitimate mobile station.

Home Location Register (HLR) -The location register or database to which a MIN is assigned for record purposes such as subscriber information.

Internati nal Mobile System Identification (IMSI) - The information which uniquely identifies a subscriber to the PSTN or PLMN.

Mobile Identification Number (MIN) - The 10-digit number that represents the phone number of the subscriber unit.

Mobile Station (MS) - The mobile or portable subscriber radio telephone equipment (same as Cellular Subscriber Station).

Mobile Switching Center (MSC) - A configuration of equipment that provides cellular radiotelephone service.

National Number - The number identifying a subscriber line or terminal within an area designated by a country code.

Network - The telecommunications equipment that has any part in processing a call or a supplementary service for the subscriber referred to. It may include local exchangers and transit exchanges, but does not include the mobile station and is not limited to the "public network" or any other particular set of equipment.

NDSS - Network Directed Systems Selection

Numeric Assignment Module (NAM) - The electronic memory module of the subscriber unit where the MIN and other subscriber specific parameters are stored. Subscriber units that have multi-NAM features offer users the option of using their units in several different markets by registering with a local number in each location.

OTASP - Over-the-Air Sevice Provisioning

PCS - Personal Communication Services

Personal Identification Number (PIN) - A string of digits used to validate a subscriber's identity. In order to distinguish the PIN from the de-registration or de-activation feature codes using a Modifier Digit "0," the PIN shall not start with the digit 0. The PIN shall be at least 4 digits and shall not have too many repeated digits. (e.g., no more than 2).

Portability - The ability for a smart card to operate in a variety of smart card compatible terminals.

PLMN - Public Land Mobile Network

PSTN - Public Switch Telephone Network

Registration - Method by which a mobile station notifies the network of its location and parameters.

Roamer - . A mobile station operating in a cellular system or network other than the one from which service is subscribed.

Roamer Service Profile - . The specific set of features, capabilities and/or operating restrictions, other than financial accountability, associated with the subscriber.

Service Provider - A company, organization, business, etc. which sells, administers, maintains, and charges for the service. The service provider may or may not be the provider of the network.

Shared Secret Data(SSD) - A 128-bit pattern stored in the mobile station (in semi-permanent memory) and known by the network. The SSD is a concatenation of two 64-bit subsets: SSD_A which is used to support the authentication procedures and SSD_B which serves as one of the inputs to the process generating the encryption mask.

Subscriber Identification Module (SIM) - The SIM card is the Subscriber Identity Module. It contains necessary information to verify and authenticate the subscriber. There are two sizes, full size and plug-in.

Smart Card Serial Number - In order for the service providers to identify the smart card, there needs to be a smart card serial number. This is a unique number that identifies the smart card. It can be printed on the card. It is not secret data, it is not sent over the air.

Stage 1 - This stage is part of the overall method used to characterize telecommunication services. Stage 1 defines the service aspects of a capability. Specifically, Stage 1 provides a service description of a telecommunication service from the user point of view (refer to *CCITT Recommendation I.130).*

Stage 2 - This stage is part of the overall method used to characterize telecommunication services. Stage 2 defines the functional aspects of a capability. Specifically, Stage 2 provides a description of the functions at the user-network interface

and inside the network between network elements (refer to *CCITT Recommendation I.130).*

Stage 3 - This stage is part of the overall method used to characterize telecommunication services. Stage 3 defines the network implementation aspects of a capability. Specifically, Stage 3 provides a description of the actual protocols and formats used to develop the telecommunication service (refer to *CCITT Recommendation I.130).*

Subscriber - A person authorized for a feature or service.

Subscriber unit (SU) - The portion of the mobile or portable subscriber radiotelephone equipment that contains the unique information to identify a subscriber. The SU can be the entire mobile station itself, or a smart card or other device that contains such information.

Universal Identification Module (UIM) - This term is used in T1P1.3 to refer to the logic function or the SIM card in the mobile station.

World Numbering Plan - A plan created by the CCITT that provides each telephone subscriber with a unique number. Each world telephone number consists of a country code followed by the national number as defined in *CCITT Recommendations E.164.* By international agreement, the number of digits in the country code plus national number is limited to a tOTASPI of 12 digits currently, with a recommendation to increase the maximum length to 15 digits by the end of 1996.

Validation - The process by which a subscriber is authorized to access and use a cellular network.

Verification - The method used by a service provider to determine the credit of a new subscriber.

4. Global Feature Description

Upon the receipt of a smart card from a service provider, the subscriber shall be responsible for inserting the smart card into a mobile station or a smart card compatible device.

The subscriber with a smart card may have to subject to Card Holder Verification (CHV) (e.g. use of a Personal Identification Number - PIN) in order to access voice/data applications. Each smart card shall have a CHV to secure card access. Use of CHV is implementation specific.

The subscriber may use a single smart card containing multiple applications in multiple smart card compatible devices, provided the device supports the particular application. For example, a multi-application card supporting a telephony and a banking application may be successfully used in both a mobile station and an ATM-type machine.

The smart card can be removed from the mobile station when not in use. The size of a smart card does not have to be smaller than the mobile station as long as a compatible interface is provided. Full size smart cards are preferred because they can be removed from the mobile station and stored elsewhere with other payment type cards and used for other horizontal applications.

A normal phone call should not be allowed without the smart card present in the mobile station. There are exceptions to this case which will be determined and authorized by the

service provider. Examples are emergency 911 calls, calls to update the value of the individual account, 800 calls, service order calls, etc. When the smart card is inserted, the mobile station can be powered up manually or automatically.

It is assumed one card per subscription in this document.

5. Smart Card Feature Descriptions

The following sections describe individual smart card features and services.

5.1. Pre-paid Service

Pre-paid subscription will provide an attractive payment option to service providers as well as to a large segment of the customers because it can provide a means for "cash economy" and for poor credit, high risk customers to obtain wireless service.

A smart card can be used to support pre-paid subscription similar to a debit card. The subscriber can pay cash or link the smart card to an authorized credit card institute. The activation of smart card can be done at home through phone via OTA, at an ATM machine, at a service center or other convenient stores equipped with the appropriate, secured terminal. The distribution of the smart card can be handled through regular mail, so can the "refill" mechanism.

A unit amount, in dollars or minutes, representing purchased air time may be stored on a smart card. The user may make and receive phone calls, and use network services. The value on the smart card will be decremented as the authorized subscriber makes phone calls until the value of the card is exhausted. The subscriber may replenish the card by purchasing additional units. The service provider may offer a variety of rate plans and provision the smart card according to the subscriber's choice. After provisioning, the card value can only be decremented as phone calls are made.

The value of the card can only be incremented through an authorized party or process to avoid illegal tempering. The value filled in the smart card can be re-adjusted per subscriber's request through the pre-arranged authorization process supported by the service provider.

The smart card may be used to track value off-line, i.e. without network involvement. The subscriber may request to have balance and other relevant call detailed records displayed in the window provided on a mobile station.

Once the value on the smart card is depleted, the customer can not make normal phone calls except specified by the service provider. These allowable free calls can include 911 emergency calls, 800 calls, or subscription related calls such as 411, 611, etc. to update the value and privileges carried by the card subscriber.

The smart card provisioning process, i.e., subscriber provisioning has to be automated with sufficient tools (OTASP and/or SIM application toolkit) to warrant an operation above and beyond the conventional existing plastic calling cards with or without the magnetic stripes. Manual operations to update individual subscriber databases are not acceptable by the service provider.

A subscriber scenario is described as follows: An automated kiosk at a neighborhood convenience store may accept cash, debit or credit cards in payment for added telecom units. The subscriber inserts cash or swipes a debit or credit card, indicates the value of the purchase, then receives a smart card for equal replenishment. Alternatively, the subscriber's service may be call-diverted to a customer service representative for the purchase of additional units. The customer service representative may replenish the smart card value via Over-the-Air Service Provisioning administration, or other automated procedures. The service provider can also mail the smart card to the subscriber for a newly established amount and a feature set.

The Pre-Paid Service should allow the service provider to better administer customer credit control, mass market penetration and acceptance of temporary or short term subscribers. This capability should make it possible for service providers to implement various billing strategies, such as mobile originated or mobile terminated limitations, as well as subscriber deletion without making major modifications to their networks. Eventually the smart card should carry individual billing information such as advice of charge.

Initially, a simplified Pre-paid Service with minimum impact on the network should be made available for the service provider to offer this service quickly. Later, a full capability of the Pre-paid service should be accommodated. This full capability is characterized as follows:

The residual value on a smart card should be dealt with fairly. A message should be delivered to the subscriber indicating insufficient value to make the next call. Options should be informed.

Examples of optional steps can be:

1. Call the service center to receive changes;

2. Call the service center to grant more value;

3. Enter a card terminal to receive value equivalent to additional cash payment;

4. Authorize usage of credit account to extend usage;

5. Receive a new card from a service center or in mail.

These options will be adopted according to the type of smart card as explained below:

1. Throwaway smart card. After credit amount and/or time expires, the smart card is permanently disposed of for making phone calls.

2. Rechargeable smart card. The service provider can define circumstances by which customers are able to recharge their smart cards with additional payments.

3. Upgrade from prepaid to credit card. This will allow the subscriber to use post payment service as it is typically the case after completing a successful credit check.

Some tentative attributes and anticipated values are provided below:

Attribute	Value
Account balance	**Assume $0 - $10,000, allowable per Service Provider**
Rate set preferences	**Assume maximum 100 rate plans**
Accumulative call meter	
Advice of charge	
Currency exchange rate	**Exchange rate of major currencies**
OTASP	**Over the Air Service Provisioning**
DMH link	**Tie to the near real time billing data**
CHV Authorization	**CHV, ESN and MIN combination**

5.1.1. Normal Procedures With Successful Outcome

5.1.1.1. Authorization

Pre-paid Service may be provided after pre-arrangement with the service provider, or may be made generally available by the service provider.

5.1.1.2. De-Authorization

If Pre-paid Service is provided after pre-arrangement with the service provider, the service shall be de-authorized at the subscriber's request or for administrative reasons.

5.1.1.3. Registration

Pre-paid Service should allow registration of the smart card either through the terminal/mobile station or through the network.

5.1.1.4. De-Registration

Pre-paid Service does not have to have De-Registration.

5.1.1.5. Activation

Pre-paid Service shall be activated upon authorization.

5.1.1.6. Deactivation

Pre-paid Service shall be de-activated upon De-Authorization.

5.1.1.7. Invocation

Pre-paid Service is invoked by issuing of the appropriate application level commands.

5.1.2. Exception Procedures or Unsuccessful Outcome

If the card is warped or damaged, the card can not trigger any service, replacement will be sought. If card access by an unauthorized user is detected through CHV or other security verification, the call will be denied.

5.1.2.1. Registration

None identified.

5.1.2.2. De-Registration

None identified.

5.1.2.3. Activation

None Identified.

5.1.2.4. Deactivation

None Identified.

5.1.2.5. Invocation

If Pre-paid Service cannot be established for the service session or if the service sessions are interrupted in progress, the network may clear the service session. The originator of the service session should be provided with an indication that the service session has failed.

5.1.2.6. Exceptions While Roaming

None identified.

5.1.2.7. Exceptions During Intersystem Hand-off

Intersystem hand-off should not affect Pre-paid Service integrity.

5.1.3. Alternate Procedures

None identified.

5.1.4. Interactions With Other Wireless Services

5.1.4.1.

For Further Study

5.2. Plastic Roaming Service

Plastic Roaming Service will allow a user to roam outside of his/her home system through the use of a smart card. This service will provide the capability of allowing the user to authenticate with a preferred roaming system which has been previously defined on the smart card.

The smart card will contain a list of preferred serving systems that would associate the name/greeting of the service provider the subscriber is roaming on. When a subscriber selects a preferred serving system, the name and greeting of the local service provider may be delivered to the subscriber. This list will provide the subscriber greater flexibility of maintaining his/her most frequently visited location.

A smart card service provider may issue provided support of mutilple technology imprinted on the card. The service provider that has more than one type of technology to offer to its cellular or PCS subscribers will have the capability of providing extended roaming access on the same smart card. If a smart card subscriber is unable to access a particular network technology, he/she may chose to disconnect from the network and reconnect with another network technology.

The smart card must be inserted into a smart card terminal unit at all times while plastic roaming. The smart card prepersonalization data must be verified and validated before plastic roaming can occur. After registeration the service provider may access the roamer service profile. The roamer service profile may store and maintain the specific feature information (e.g. automatic roaming, NDSS, etc.) for call origination and termination

Smart card location information and time of call would provide geographical roaming information for call origination and termination. These characteristics should be use to facilitate billing functions via the home service provider.

Ultimately, the smart card should allow roaming across multiple bands (800, 900, 1800, 1900 MHz, etc.) and multiple access technologies (PCS, CDMA, GSM, AMPS, TDMA etc.)

Attribute	Value
Prepersonalization data	**Authentication key, IMSI, status of card(block, unblock), CHV**
IMSI	**International Mobile Station Identification**
TMSI	**Temporary Mobile Station Identification**
LAI	**Location Area Information (SID/NID)**
Time	**Time related to periodic location updating**
Roamer Service Profile	**Automatic roaming, SSPR, NDSS, CW, CFB, 3WC, etc.**
Extended Network Technology Access	**Provide interoperability with other networks (GSM, CDMA, PCS, AMPS, TDMA)**
OTASP	**Over the Air Service Provisioning**
SID/NID	**List of preferred Systems/Network ID provided by the home system**
Feature Codes	**Automatic roaming, SSPR, NDSS**

5.2.1. Normal Procedures With Successful Outcome

5.2.1.1. Authorization

Plastic Roaming Service may be provided after pre-arrangement with the service provider, or may be made generally available by the service provider. The smart card subscriber prepersonalization data would be imprinted on the card at authorization.

5.2.1.2. De-Authorization

If Plastic Roaming Service is provided after pre-arrangement with the service provider, the service shall be de-authorized at the subscriber's request or for administrative reasons.

5.2.1.3. Registration

Plastic Roaming Service has no registration. The mobile station handles registration.

5.2.1.4. De-Registration

Plastic Roaming Service has no De-Registration.

5.2.1.5. Activation

Plastic Roaming Service shall be activated upon authorization.

5.2.1.6. Deactivation

Plastic Roaming Service shall be de-activated upon De-Authorization.

5.2.1.7. Invocation

Plastic Roaming Service is invoked by the smart card user inserting the smart card into the mobile station or smart card compatible device. The user may enter a CHV for verification to access the smart card roamer service profile and other applications.

5.2.2. Exception Procedures or Unsuccessful Outcome

5.2.2.1. Registration

None identified.

5.2.2.2. De-Registration

None identified.

5.2.2.3. Activation

None Identified.

5.2.2.4. Deactivation

None Identified.

5.2.2.5. Invocation

If Plastic Roaming Service cannot be established for the service session or if the service sessions are interrupted in progress, the network may clear the service session. The originator of the service session should be provided an indication that the service session has failed.

5.2.2.6. Exceptions While Roaming

If plastic roaming service cannot be established or a service session fails while roaming, the originator has the option of reconnecting to another extended network technology. Reconnection would occur after the originator has disconnected from the current extended network technology he/she is on and re-register with another extended network.

5.2.2.7. Exceptions During Intersystem Hand-off

Intersystem hand-off should not affect Plastic Roaming Service integrity.

5.2.3. Alternate Procedures

None identified.

5.2.4. Interactions With Other Wireless Services

5.2.4.1.

For Further Study

5.3. Fraud Prevention Service

The smart card provides mechanisms that assure a high degree of privacy and authentication. This privacy and authentication function is the basis for all other smart card services. This function should be compliant with the existing UIM authentication and privacy specification for the PCS applications (ref. T1P1.3.)

The Fraud Prevention Service provides the following measures:

1. Preventing cloning of subscriptions by:
   - Securing the distribution of subscriber data
   - Secure storage on the smart card
   - No programming of phone (at distribution) with sensitive data

2. Authentication:
   - User to SIM (subscription) with CHV/PIN
   - SIM (subscription) to network with secret keys and algorithms

3. Safeguarding subscriber anonymity because:
   - The average interceptor cannot tell who is using the phone (TIMSI), nor can the interceptor track the user.

4. Encryption of:
   - all signaling data and
   - all communications content (voice, data, etc.)

The smart card will handle multiple security algorithms including IS-41 and GSM based algorithms.

The smart card will be used in conjunction with the conventional CHV code. Subscriber fraud should be drastically reduced with the smart card due to the fact that the keys and the algorithm execution is performed within a secure environment of a single chip. At no time does secret data or intermediate algorithmic results leave this secure environment.

The smart card authentication will be handled either by the network or the compatible terminal/mobile station. The smart card needs to operate with networks that can/will handle authentication as well as those that can/will not. Depending on the network authentication capability, the proper combination of the CHV, A-key, MIN (or IMSI) and the ESN of the mobile station will be validated for a particular subscriber to assure maximum authentication. The subscriber security identity is portable with the card and the subscriber across all smart card capable mobile stations.

The smart card will enable the service provider to process authentication key with secured distribution and management. It should complement security functions supplied by the OTASP.

Attribute	Value
Authentication key **Authentication algorithm** **OTASP authentication responses**	

1

2

3 ## 5.3.1. Normal Procedures With Successful Outcome

4 ### 5.3.1.1. Authorization

5 Fraud Prevention Service may be provided after pre-arrangement with the service
6 provider, or may be made generally available by the service provider.

7 The three categories of Fraud Prevention may be authorized as follows:

8 1. CHV code, is initially always enabled. The user can disable and enable this service at
9 will. However pre-paid cards will always need a CHV code before attempting a call
10 setup. The CHV will be administrated by the service provider in conjunction with
11 different levels of security. The subscriber can access and change only the CHV, not
12 other security algorithms involving A-key, etc.

13 2. Authentication is mandatory. The A-key or similar parameters may be stored on a
14 UIM together with an authentication algorithm.

15 3. Encryption prevents subscription data from being illegally captured and used.
16 Encryption shall always be used whenever available.

17 ### 5.3.1.2. De-Authorization

18 If Fraud Prevention Service is provided after pre-arrangement with the service provider,
19 the service shall be de-authorized at the subscriber's request or for administrative
20 reasons. The Fraud Prevention Service is provided until termination of entire telephone
21 service at the subscriber's request or for administrative reasons.

5.3.1.3. Registration

Fraud Prevention Service has no registration.

5.3.1.4. De-Registration

Fraud Prevention Service has no De-Registration

5.3.1.5. Activation

Fraud Prevention Service shall be activated upon authorization.

5.3.1.6. Deactivation

Fraud Prevention Service shall be de-activated upon De-Authorization.

5.3.1.7. Invocation

Fraud Prevention Service is invoked by issuing of the appropriate application level commands.

The three categories Fraud Prevention will be invoked:

1. CHV code is invoked by issuing of the appropriate application level commands.

2. Authentication is invoked by the MS or by the network.

3. Encryption is invoked by issuing of the appropriate application level commands.

5.3.2. Exception Procedures or Unsuccessful Outcome

5.3.2.1. Registration

None identified.

5.3.2.2. De-Registration

None identified.

5.3.2.3. Activation

None Identified.

5.3.2.4. Deactivation

None Identified.

5.3.2.5. Invocation

If Fraud Prevention Service cannot be established for the service session or if the service sessions are interrupted in progress, the network may clear the service session, The originator of the service session should be provided an indication that the service session has failed.

5.3.2.6. Exceptions While Roaming

None identified.

5.3.2.7. Exceptions During Intersystem Hand-off

Intersystem hand-off should not affect the Fraud Prevention Service integrity.

5.3.3. Alternate Procedures

None identified.

5.3.4. Interactions With Other Wireless Services

5.3.4.1.

Fraud Prevention Service is the foundation block to all the other services. This service will interact with other services at the beginning of the call set-up. More study is necessary.

5.4. Future Services

5.4.1. Portable Storage Service

Mapping of feature codes and other subscriber specific data to more user-friendly interface can be done in the smart card. Data stored in the smart card can be carried with the subscriber for activation in other location, device, or network. Examples of these data are listed below:

1) Translation of 911 to the number appropriate for a specific geographic location.

2) Service provider's name/greeting associated with certain SID/NID. When subscriber places a call in a new SID/NID, name and greeting of the local service provider can be delivered to the subscriber.

3) Voice print of the subscriber.

4) Audio characteristics.

5) Short messages, voice and facsimile messages delivered to the subscriber.

6) Personal health data, education and entertainment preferences.

7) Business specific application of data per employee, e.g. dispatch route assignments for driver X, etc.

Attribute	Value
Feature codes	
SID/NID list	
Voice print	
Audio signature	
Short messages	
Voice messages	
Facsimile messages	
Route information	
Personal health record	
Entertainment data	
OTASP	
CHV	

5.4.2. Non-telephony Services

Many current and proposed smart card applications address industries and consumer needs outside of telephony. A link to these services can be provided by the smart card which will allow telephony and non-telephony applications to co-exist on the same card. For example:

1) Transparent wireless transport for "end-to-end" applications facilitating interaction between the smart card and another entity, e.g. a host machine.

2) Business alliance between financial institution and the wireless service provide can link telephony and credit services via the smart card.

A telephony application on the smart card may provide wireless access to supply communication needs of another application also on that smart card. However, a number of these applications rely upon some form of transport to enable communications with a host application or database. For example, a financial services smart card enabling banking transactions might require access to host applications for funds transfer, payment and account updates. A multi-application smart card containing both a financial services and wireless services application could provide the required communications transport services. The user inserts the smart card into the mobile station, enters the appropriate CHV, then selects the desired financial services application from an application menu. User information and transaction data could be transmitted via SMS , voice or data channel from the smart card to the recipient application and vice versa. The user physically interacts only with the mobile station.

Attribute	Value
Application name	
Transport protocol	
CHV	
Application detailed billing	
SMS	